Incident Final Report

Executive Summary:

On December 28, 2022, at 7:20 p.m. PT, our organization experienced a security breach where an unauthorized individual accessed sensitive customer data, including Personally Identifiable Information (PII) and financial records. The breach affected approximately 50,000 customer records, and the estimated financial impact is $100,000 in direct losses and potential revenue impact. The incident has been thoroughly investigated and resolved.

Incident Timeline:

At 3:13 p.m. PT on December 22, 2022, an employee received an email from an external source. The sender claimed to have stolen customer data and demanded a $25,000 cryptocurrency payment to keep the data from being released. The employee dismissed the email as spam and deleted it.

On December 28, 2022, the same employee received a follow-up email from the same sender, which included a sample of the stolen data. This time, the demand was increased to $50,000. Upon receiving this second email, the employee notified the security team, which initiated an investigation. From December 28 to December 31, 2022, the security team focused on determining the extent of the data theft and how the breach occurred.

Investigation Findings:

The security team arrived on-site to conduct a full investigation. The root cause of the breach was identified as a vulnerability in the organization's e-commerce web application. This flaw allowed an attacker to perform a forced browsing attack by manipulating the order numbers in the URL of purchase confirmation pages, which gave them access to customer transaction data.

Upon confirming the web application vulnerability, further analysis of the access logs showed that the attacker had retrieved thousands of customer purchase records.

Response and Remediation:

The organization worked closely with the public relations team to inform customers about the data breach. Affected customers were offered free identity protection services to mitigate potential risks from the data leak.

Reviewing the web server logs revealed the attack's full extent, showing a high volume of sequential customer order requests from a single source.

Recommendations for Future Prevention:

To prevent similar incidents in the future, the following measures are recommended:

- Regular vulnerability scans and penetration tests.
- Improved access control mechanisms, including:
  - Implementing allowlisting to restrict access to specific URLs and automatically block unauthorized requests.
  - Ensuring that only authenticated users can access sensitive content.